National student Loan Data System (NSLDS)
Corrective Action Plan,
September 2000

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
1	Identification and Authentication	There was no evidence of policies for defining the password management process, or procedures for monitoring it, nor was there any evidence that previous discrepancies had been addressed. Users share accounts and passwords. Password expiration interval was increased to 120 days.		Ensure NSLDS complies with SFA standards for data user IDs and passwords. See the Identification and Authentication Section above for detailed guidance.		
2	System Interconnection/ Information Sharing	Despite the numerous interfaces to NSLDS, system managers do not feel MOUs or MOAs are applicable.		Ensure all NSLDS connections and information sharing with non-SFA entities are codified. See the section above on system interconnection and information sharing for further details.		
3	Security Life Cycle Planning	While security in the NSLDS life cycle was reported to be described in the system security plan, a copy of this plan was not provided.		Ensure that (as appropriate) privacy and security in the information life cycle are addressed in NSLDS life cycle planning documents. See the Security Life Cycle Planning section for additional details.		
4	Authorize Processing	Although NSLDS has not sought certification, this report could serve as the basis for a system certification/ authority to operate.		Obtain an IATO for one year from the OCIO as soon as practical. Within eighteen months from issuance of the IATO, perform a formal NSLDS certification test under NIST guidance (FIPS 102).		
5	Production, Input/Output Controls	There was no evidence of controls for the installation and use of the application.		Implement Security Life Cycle Planning, Authorize Processing and Application Software Maintenance Control recommendations; document input/output controls in the NSLDS security plan.		

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
6	Security Awareness and Training	The description of training provided on an "as needed" basis is only marginally adequate, and suggests that NSLDS opts out of annual security and privacy training.		Provide security training for the NSLDS SSO; once trained, the NSLDS SSO should assist the OCIO in setting up an entity-wide security awareness and training program. See the Security Awareness and Recommendations sections for detailed guidance.		
7	Central Security Focus/ Assigned Responsibility	ACSO is not a full-time position. ACSO has not received technical training regarding NSLDS security. Data ownership has not been defined clearly. CSO and ACSO were not involved directly in addressing certain key decisions affecting the NSLDS security. Provisions of the Department's security and procurement policy were not followed in awarding NSLDS contract.		Ensure the CBS SSO is properly trained and qualified. See the section on security training and awareness, and the related recommendations for the Promote Awareness phase of the risk management cycle. In addition, a long-term computer security strategy, a compliance program, and descriptions of any liaison function for either external or intraorganizational entities should be documented.		
8	Documentation	While CBS does maintain a substantial body of system documentation, several other required documents are missing. These include: • functional requirements • system test results • user rules/procedures • certification/accreditation statements/documents		Ensure the NSLDS security plan is NIST-compliant.		

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
9	Logical Access Controls	Previous year audits indicate NSLDS needed to tighten up on some areas of logical access (see red text below). Evidence made available does not indicate these weaknesses have been addressed, nor was enough information provided to allow an assessment of the NSLDS logical access posture. RACF is used to control a role-based access schema, but the granularity of access that can be achieved was not discussed. There is no formal process for removing terminated employees or employees who no longer need the access. NSLDS school users can view all loans and borrower transactions of a student via the SSN search regardless of whether or not the school was authorized by that student in his/her Free Application For Federal Student Aid (FAFSA) form. Changes to the NSLDS were not announced in the Federal Register. RACF system default UserID was not revoked. Security changes to the NSLDS mainframe by users with the system or group SPECIAL attribute are not reviewed by designated personnel.		Document and implement within one year NSLDS-specific policies, standards, procedures and guidelines to govern logical access processes and mechanisms.		

No	Control Area	Observation	Concur with Observation	Corrective Action / Description	Completion Date	Point of Contact
10	Audit Trails	Previous year audits indicate that NSLDS needed to tighten up on some areas of auditing and monitoring (see red text below). Evidence made available does not indicate that these weaknesses have been addressed, nor was enough information provided to allow an assessment of the NSLDS audit and audit assessment posture. RACF is used to record auditable events, but the granularity of audit that can be achieved was not discussed, nor were procedures for reviewing audit records. No audit tool is available to monitor the SSN search activities. NSLDS audit review is not performed on a daily basis.		Ensure NSLDS audit results are being used effectively to help NSLDS managers make appropriate risk decisions. See the Audit Trails and Recommendations sections for additional details.		
11	Applicable Laws and Regulations	CBS is cognizant of applicable laws and regulations. Regarding the Privacy Act: although this system presumably complies with notice, publication, and annual/biennial/quadrennial review requirements, NSLDS management did not respond to the questionnaire provided on 6 Jul 00, so the system's current compliance posture is unknown.		N/A		